



DEPARTMENT OF THE ARMY
OFFICE OF THE SECRETARY OF THE ARMY
107 ARMY PENTAGON
WASHINGTON DC 20310-0107

Office Information Officer, Chief / G-6

28 SEP 2006

SAIS-GKP

MEMORANDUM FOR SEE DISTRIBUTION

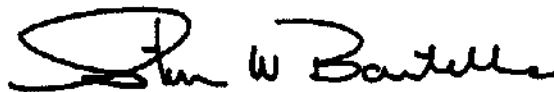
SUBJECT: Army Data-At-Rest (DAR) Protection Strategy

1. In light of current events and the resulting loss of sensitive information, it is imperative that the Army immediately initiate several actions to protect Army data at rest. Army policy, standards, and guidance have existed since 2003 and relied on voluntary management enforcement. Army approved DAR products are identified, but are not deployed Army-wide and are implemented as the local Command can fund, acquire, and integrate. I am now directing the immediate implementation of DAR remediation procedures for all mobile Information Systems (ISs).
2. The following concurrent actions will focus Army efforts on remediation of sensitive information protection and security violations. Commanders and Designated Approving Authorities will implement the following:
 - a. Local procedures to identify and label laptops designated for travel support. Prioritize efforts to securing the most vulnerable users and systems initially. Include Universal Serial Bus device management (e.g., thumb drives), accountability and security. Ensure compliance with reporting procedures to notify leadership of loss of protected IS through appropriate privacy and incident response channels.
 - b. For those organizations with an existing DAR encryption capability, extend those capabilities to all remaining information systems where data is at risk.
 - c. For those lacking a DAR encryption capability, leverage existing Microsoft (MS) Windows XP Pro® Encrypting File System (EFS) capabilities coupled with your active directory (AD) management structure to enable file encryption through a centrally managed EFS certificate issuance. A DAR best business practice (BBP) with technical guidance and standards will be published on the EFS capabilities in the form of a DAR BBP and available in October 2006.
 - d. For those lacking a MS EFS and AD environment; as described in the "Road Warrior" Laptop Security BBP, ensure that approved solutions and standards are used for protecting DAR on all mobile ISs. This will be accomplished either by using "whole disk" encryption tools or "file system" encryption tools for sensitive or protected information (currently Credant and PointSec are approved for use in the Army).

SAIS-GKP

SUBJECT: Army Data-At-Rest (DAR) Protection Strategy

3. Simultaneously, the Army CIO/G6 will be evaluating an initial Headquarters Department of the Army DAR implementation and will use these results to drive the requirements and business case analysis for the acquisition of an interim enterprise solution that addresses DAR encryption for all users and systems NLT 1 January 2007.
4. Finally, to achieve the Army end-state of a Department of Defense (DOD) Common Access Card-integrated solution, we will actively assist the Office of the Secretary of Defense to ensure a seamless, integrated, and comprehensive enterprise solution is provided in calendar year 2007.
5. My point of contact for this action is Mr. Gary L. Winkler, Principal Director, Governance, Acquisition and Chief Knowledge Officer, comm: 703-602-9316, e-mail: gary.winkler@us.army.mil.



STEVEN W. BOUTELLE
Lieutenant General, GS
Chief Information Officer/G-6

DISTRIBUTION:

PRINCIPAL OFFICIALS OF HEADQUARTERS, DEPARTMENT OF THE ARMY

COMMANDER

U.S. ARMY EUROPE AND SEVENTH ARMY
EIGHTH U.S. ARMY
U.S. ARMY FORCES COMMAND
U.S. ARMY TRAINING AND DOCTRINE COMMAND
U.S. ARMY MATERIEL COMMAND
U.S. ARMY CORPS OF ENGINEERS
U.S. ARMY SPECIAL OPERATIONS COMMAND
U.S. ARMY PACIFIC
U.S. ARMY MILITARY TRAFFIC MANAGEMENT COMMAND
U.S. ARMY CRIMINAL INVESTIGATION COMMAND
U.S. ARMY MEDICAL COMMAND
U.S. ARMY MILITARY DISTRICT OF WASHINGTON
U.S. ARMY SPACE AND MISSILE DEFENSE COMMAND

SUPERINTENDENT, U.S. MILITARY ACADEMY